

## REMARKS

Applicant requests favorable reconsideration and allowance of this application in view of the foregoing amendments and the following remarks.

Claims 4-6 and 14-17 are pending in this application, with Claims 4, 14 and 17 being independent.

Claims 4, 14, and 17 have been amended. Applicant submits that support for the amendments can be found in the original disclosure. No new matter has been added.

Claims 4, 14, and 17 were rejected under 35 U.S.C. 112, second paragraph, as failing to set forth the subject matter which applicant(s) regard as their invention. Applicant submits that those claims have been amended in view of the Examiner's comments, and Applicant submits that the basis of the rejection has been overcome. Favorable reconsideration and withdrawal of this rejection are requested.

Claims 4-6 and 14-17 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,711,677 (Wiegley) in view of U.S. Publication No. 2005/0097323 (Lapsun et al.). Applicant respectfully traverses this rejection for the following reasons.

As recited in independent Claim 4, the present invention includes, *inter alia*, the features of generating a common key based on a print ID transferred from an image data processing device, transmitting the common key to the image data processing device, analyzing print control data transmitted from the image data processing device to extract from the print control data print image data that has been forgery-preventing-image-processed, encrypted, and converted into a command in the image data processing device, and decrypting the extracted print image data, wherein the print image data has been

forgery-preventing-image-processed and encrypted in the image data processing device using the common key received from the image data recording device.

With these features, print image data that has been forgery-preventing-image-processed and encrypted in an image data processing device using a common key generated by the image data recording device can be extracted from print control data and decrypted in the image data recording device using the common key. It is thereby possible for the image data recording device to ensure that it prints only forgery-prevention-image-processed image data. Applicant submits that the cited art fails to disclose or suggest at least the above-mentioned features of Claim 4.

Wiegley discloses an encryption security system for printer client/printer communications that reduces or eliminates the risk of replay attacks. The validity of a secure print job is determined using a public/private key pair. The printer client encrypts print data using the public key of the public/private key pair or, preferably, a session key. If the print job is determined to be valid, then the printer decrypts the print data and prints the data. (See abstract.)

However, Applicant submits that Wiegley fails to disclose or suggest at least the feature of analyzing print control data to extract from the print control data print image data that has been forgery-preventing-image-processed, encrypted, and converted into a command in an image data processing device, wherein the print image data has been forgery-preventing-image-processed and encrypted in the image data processing device using a common key received from an image data recording device. Applicant further submits that the other cited art fails to remedy the deficiencies of Wiegley.

For the foregoing reasons, Applicant submits that the present invention recited in independent Claim 4 is patentable over the art of record.

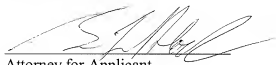
Independent Claims 14 and 17 recite features similar to those of Claim 4 discussed above, and those claims are believed to be patentable for reasons similar to Claim 4.

The dependent claims are believed to be patentable for at least the same reasons as the independent claims, as well as for the additional features they recite.

In view of the above amendments and remarks, the claims are now in allowable form. Therefore, early passage to issue is respectfully solicited.

Applicant's undersigned attorney may be reached in our Washington, D.C. office by telephone at (202) 530-1010. All correspondence should continue to be directed to our below-listed address.

Respectfully submitted,



Attorney for Applicant

Brian L. Klock

Registration No. 36,570

FITZPATRICK, CELLA, HARPER & SCINTO  
30 Rockefeller Plaza  
New York, New York 10112-3801  
Facsimile: (212) 218-2200  
BLK

FCHS\_WS 1467313v1